Your search matched **3** documents.

A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 **Field inversion and point halving revisited**
Fong, K.; Hankerson, D.; Lopez, J.; Menezes, A.;
Computers, IEEE Transactions on ,Volume: 53 , Issue: 8 , Aug. 2004
Pages:1047 - 1059

[Abstract] [PDF Full-Text (776KB)] **IEEE JNL**

2 **Reducing elliptic curve logarithms to logarithms in a finite field**
Menezes, A.J.; Okamoto, T.; Vanstone, S.A.;
Information Theory, IEEE Transactions on ,Volume: 39 , Issue: 5 , Sept. 199
Pages:1639 - 1646

[Abstract] [PDF Full-Text (648KB)] **IEEE JNL**

3 **A semiflash A/D ultra-fast conversion technique**
de Menezes, A.S.C.; de Avilez Filho, O.V.;
Electrotechnical Conference, 1991. Proceedings., 6th Mediterranean , 22-24 M
1991
Pages:323 - 326 vol.1

[Abstract] [PDF Full-Text (152KB)] **IEEE CNF**

Google

Web Images Groups[New!] News Froogle more »

knudsen "point halving" Search Advanced Search Preferences

Web

Results **1** - **10** of about **74** for **knudsen** "**point halving**". (**0.05** seconds)

[PDF] The Cryptographic Marriage of (Georg) Frobenius and **Point Halving**
File Format: PDF/Adobe Acrobat - View as HTML
... of (Georg) Frobenius and **Point Halving** Officiant: Roberto Avanzi (Witnesses: Mathieu Ciet and Francesco Sica) ... Koblitz Curves **Point Halving** Superstition ...
www.arehcc.com/download/Crypto_Marriage.pdf - Similar pages

Field Inversion and **Point Halving** Revisited
... We present a careful analysis of elliptic curve point multiplication methods that use the **point halving** technique of **Knudsen** and Schroeppel and compare these ...
csdl.computer.org/comp/trans/tc/2004/08/t1047abs.htm - 13k - Cached - Similar pages

CACR: 2001 Conferences
... fields of small characteristics Robert Harley: Generating secure elliptic curves using the AGM and early abort strategies Erik **Knudsen**: **Point halving**-How it ...
www.cacr.math.uwaterloo.ca/ conferences/2001/ecc/announcement.html - 15k - Cached - Similar pages

[PDF] Field inversion and **point halving** revisited
File Format: PDF/Adobe Acrobat - View as HTML
... The final section presents a careful analysis of point multiplication methods that use the **point halving** technique of **Knudsen** and Schroeppel, and compares ...
www.cacr.math.uwaterloo.ca/ techreports/2003/corr2003-18.pdf - Similar pages
[More results from www.cacr.math.uwaterloo.ca]

Elliptic Scalar Multiplication Using **Point Halving**
... Elliptic Scalar Multiplication Using **Point Halving**. Source, Lecture Notes In Computer Science; Vol. ... Erik Woodward **Knudsen**, Publisher, Springer-Verlag London, UK. ...
portal.acm.org/citation.cfm?id=647095.716851 - Similar pages

DBLP: Erik Woodward **Knudsen**
... ACISP 2004: 478-491. 1999. 1, Erik Woodward **Knudsen**: Elliptic Scalar Multiplication Using **Point Halving**. ASIACRYPT 1999: 135-149. Coauthor Index. ...
www.informatik.uni-trier.de/~ley/ db/indices/a-tree/k/Knudsen:Erik_Woodward.html - 3k - Cached - Similar pages

Elliptic Curve Cryptography
... Elliptic scalar multiplication using **point halving**, E. **Knudsen**, Proc. of Asiacrypt'99, Springer-Verlag, LNCS 1716, pp.135-149, 1999. (local copy); Speeding ...
cnscenter.future.co.kr/crypto/algorithm/ecc.html - 54k - Cached - Similar pages

[PDF] SCALAR MULTIPLICATION ON KOBLITZ CURVES USING THE FROBENIUS ...
File Format: PDF/Adobe Acrobat - View as HTML
... **Knudsen** [8] and Schroeppel [16] independently proposed a technique to speed up ... multiplication on all elliptic curves over binary fields based on **point halving**. ...
www.wits.ac.za/helmut/pdffiles/tauext.pdf - Similar pages

Mathematics of Computation
... 6. EW **Knudsen**, Elliptic scalar multiplication using **point halving**, Advances in Cryptology-ASIACRYPT'99 (KY Lam, E. Okamoto, and C. Xing, eds.), LNCS, no. ...
www.ams.org/mcom/2005-74-249/ S0025-5718-04-01640-0/home.html - Similar pages

Mathieu CIET Home-Page
... speed-up computation on Koblitz curve combining **point halving** and endomorphism ... Vladimir Furman, Louis Granboulan, Dan Kenigsberg, Lars **Knudsen**, François Koeune ...
www.geocities.com/cietmathieu/ - 24k - Cached - Similar pages

Gooooooogle ▶
Result Page: 1 2 3 4 5 6 **Next**

knudsen "point halving" Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Google Web Images Groups[New!] News Froogle more »
odd order point supersingular elliptic halvin Search Advanced Search Preferences

Web Results **1** - **10** of about **26** for **odd order point supersingular elliptic halving**. (**0.36** seconds)

[PDF] Field inversion and **point halving** revisited
File Format: PDF/Adobe Acrobat - View as HTML
... in 32-bit increments, in **order** to more ... of affine versus projective representations of curve **points**. ... M and inversions I) for **point** additionand doublingare ...
www.cacr.math.uwaterloo.ca/ techreports/2003/corr2003-18.pdf - Similar pages

[PS] Field inversion and **point halving** revisited Kenny Fong*, Darrel ...
File Format: Adobe PostScript - View as Text
... the selection of affine versus projective representations of curve **points**. ... Let G be a **point** of **odd order** n on E ... In Section 4.3, **point halving** is used to obtain ...
www.cacr.math.uwaterloo.ca/ techreports/2003/corr2003-18.ps - Similar pages

[PDF] Fast hashing onto **elliptic** curves over fields of characteristic 3
File Format: PDF/Adobe Acrobat - View as HTML
... of a hash function that maps arbitrary messages directly onto curve **points** in such a ... Consider the tuple (P, aP, bP, cP) where P is a **point** of **order** q of an ...
eprint.iacr.org/2001/098.pdf - Similar pages

[PDF] Efficient Pairing Computation on **Supersingular** Abelian Varieties
File Format: PDF/Adobe Acrobat - View as HTML
... more efficient to use other bases, for example to write the group **order** in base ... Replacing divisors by **points**: As explained above, the **point** R can be ...
eprint.iacr.org/2004/375.pdf - Similar pages
[More results from eprint.iacr.org]

[PDF] DETERMINING THE 2 -SYLOW SUBGROUP OF AN **ELLIPTIC** CURVE OVER A ...
File Format: PDF/Adobe Acrobat
... 2 r Z, • two **points** in E(F q), of **orders** 2 n ... 3 + ax 2 + bx + c, the rational **points** of **order** 2 are ... to decide whether or not such a rational **point** exists, we ...
www.ams.org/mcom/2005-74-249/ S0025-5718-04-01640-0/S0025-5718-04-01640-0.pdf - Similar pages

[PS] O conte'udo do presente relat'orio 'e de 'unica responsabilidade ...
File Format: Adobe PostScript - View as Text
... **Orders**. ... In **order** to compute kP , the l-bit integer k is divided into h blocks K r , each one of length a = dl=he. ... if c **odd** then Set u (c \Gamma 2d (mod 4)) ...
cnscenter.future.co.kr/resource/ crypto/algorithm/ecc/lopez00overview.ps - Similar pages

Rational **Points** and Group Structure
... law exists if there is a single **point** at infinity ... cardinality of the Jacobian modulo some **odd** primes and ... field, returns the factorization of the **order** of the ...
magma.maths.usyd.edu.au/magma/htmlhelp/text1217.htm - 16k - Cached - Similar pages

[PDF] LNCS 1716 - **Elliptic** Scalar Multiplication Using **Point Halving**
File Format: PDF/Adobe Acrobat
... We will use the notation T 2 k for a **point** of **order** 2 k ... where G is a group of **odd order** and k ⩾ 1.When k = 1 we will say that the curve has minimal two ...
www.springerlink.com/index/C8YMVX998KATTKGM.pdf - Similar pages

[PDF] LNCS 2947 - A **Point** Compression Method for **Elliptic** Curves Defined ...

File Format: PDF/Adobe Acrobat
... Tr(λ) + 1. Hence whenever n is **odd**, which we ... will belong to this subgroup of large prime **order**. ... A **Point** Compression Method for **Elliptic** Curves Defined over GF ...
www.springerlink.com/index/ACYY581CA6CBAMY7.pdf - Similar pages
[More results from www.springerlink.com]

[PS] Chapter 1 Introduction to **Elliptic** Curves.
File Format: Adobe PostScript - View as Text
... is **odd** and c ... **elliptic** curves as in the corollary and with a rational **point**, the **order** of the ... 0). However I have been able to find examples only of **orders** 1 and ...
www.math.mcgill.ca/connell/public/ECH1/c1.ps - Similar pages

Google ▶
Result Page: 1 2 **Next**

odd order point supersingular ellij Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Google

Web Images Groups[New!] News Froogle more »

halving koyama okamoto "elliptic curve" Search Advanced Search Preferences

Web Results **1** - **6** of about **8** for **halving koyama okamoto "elliptic curve"**. (**0.31** seconds)

Tip: Try removing quotes from your search to get more results.

Elliptic Curve Cryptography
... Applications, N. Kunihiro and K. **Koyama**, IEICE Trans ... local copy); Realizing the Menezes-**Okamoto**-Vanstone(MOV ... scalar multiplication using point **halving**, E. Knudsen ...
cnscenter.future.co.kr/crypto/algorithm/ecc.html - 54k - Cached - Similar pages

[PS] O conte'udo do presente relat'orio 'e de 'unica responsabilidade ...
File Format: Adobe PostScript - View as Text
... discrete log problem under the Menezes-**Okamoto**-Vanstone algo ... EW Knudsen, "Elliptic scalar multiplication using point **halving**", In Asiacrypt ... [42] K. **Koyama** and Y ...
cnscenter.future.co.kr/resource/ crypto/algorithm/ecc/lopez00overview.ps - Similar pages

[PDF] A Provably Secure **Elliptic Curve** Scheme with Fast Encryption
File Format: PDF/Adobe Acrobat - View as HTML
... involves the computation of the multiple r#Q, where r has roughly the same length as n. **Koyama** et al. propose in [8] a (deterministic) **elliptic curve** RSA based ...
www-ma4.upc.es/~dgalindo/liftedRabin.pdf - Similar pages

ASIACRYPT 1999
... Kenji **Koyama**, Yukio Tsuruoka, Noboru Kunihiro: Modulus ... Imai: Optimizing the Menezes-**Okamoto**-Vanstone (MOV ... Elliptic Scalar Multiplication Using Point **Halving**. ...
www.sigmod.org/sigmod/dblp/ db/conf/asiacrypt/asiacrypt99.html - 15k - Cached - Similar pages

TOC
... **Elliptic Curve** Cryptosystems Kenji **Koyama**, Yukio Tsuruoka ... Optimizing the Menezes-**Okamoto**-Vanstone (MOV ... Scalar Multiplication Using Point **Halving** Erik Woodward ...
portal.acm.org/toc.cfm?id=647095&type=proceeding - Similar pages

[PDF] LNCS 3348 - A Provably Secure **Elliptic Curve** Scheme with Fast ...
File Format: PDF/Adobe Acrobat
Page 1. A Provably Secure **Elliptic Curve** Scheme with ... 1 Introduction Several **elliptic curve** based cryptosystems have been proposed during the last decades. ...
www.springerlink.com/index/2WLW0F8ULG0U1QXE.pdf - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 6 already displayed.
If you like, you can repeat the search with the omitted results included.

halving koyama okamoto "elliptic Search

Google Web Images Groups[New!] News Froogle more »

"efficient arithmetic on koblitz curves" Search Advanced Search Preferences

Web Results **1** - **10** of about **102** for **"efficient arithmetic on koblitz curves"**. (**0.10** seconds)

Efficient Arithmetic on Koblitz Curves
... **Efficient Arithmetic on Koblitz Curves**. Full text, Full text available on the Publisher sitePublisher Site. Source, Designs, Codes and ...
portal.acm.org/citation.cfm?id=343488 - Similar pages

A New Addition Formula for Elliptic Curves over GF(2^n)
... 7 Jerome A. Solinas, **Efficient Arithmetic on Koblitz Curves**, Designs, Codes and Cryptography, v.19 n.2-3, p.195-249, March 2000. ...
portal.acm.org/citation.cfm?id=626530.627224 - Similar pages
[More results from portal.acm.org]

[PDF] Improved Algorithms for Efficient Arithmetic on Elliptic Curves ...
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Improved Algorithms for Efficient Arithmetic on Elliptic Curves using Fast Endomorphisms Mathieu Ciet 1 , Tanja Lange 2 , Francesco ...
www.dice.ucl.ac.be/crypto/publications/2003/EC03.pdf - Similar pages

[PS] Speeding up the Arithmetic on Koblitz Curves of Genus Two
File Format: Adobe PostScript - View as Text
... 1294. Springer-Verlag, Berlin Heidelberg New York (1997) 357-371 [23] Solinas, J.: **Efficient Arithmetic on Koblitz Curves**. Techn. Report CORR 99-09, ...
www.cacr.math.uwaterloo.ca/ techreports/2000/corr2000-04.ps - Similar pages

C&O 685 - Projects
... Fast arithmetic on Koblitz curves: J. Solinas, **Efficient arithmetic on Koblitz curves**, Designs, Codes and Cryptography, 19 (2000), 195-249. ...
www.cacr.math.uwaterloo.ca/ ~ajmeneze/co485/projects.html - 11k - Cached - Similar pages
[More results from www.cacr.math.uwaterloo.ca]

Implementation
... 2000. (local copy); **Efficient arithmetic on Koblitz curves**, J. Solinas, Designs, Codes and Cryptography, 19 (2000), 195-249; Improved ...
www.securitytechnet.com/ crypto/algorithm/implementation.html - 31k - Cached - Similar pages

[PDF] SCALAR MULTIPLICATION ON KOBLITZ CURVES USING THE FROBENIUS ...
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. SCALAR MULTIPLICATION ON KOBLITZ CURVES USING THE FROBENIUS ENDOMORPHISM AND ITS COMBINATION WITH POINT HALVING: EXTENSIONS AND MATHEMATICAL ANALYSIS ...
www.wits.ac.za/helmut/pdffiles/tauext.pdf - Similar pages

[PDF] Elliptic Curve Cryptography on a Palm OS Device
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Elliptic Curve Cryptography on a Palm OS Device Andre Weimerskirch 1 , Christof Paar 2 , and Sheueling Chang Shantz 3 1 CS ...
www.crypto.ruhr-uni-bochum.de/ imperia/md/content/texte/weika_eccpalm.pdf - Similar pages

[PDF] Generic GF(2) Arithmetic in Software and its Application to ECC
File Format: PDF/Adobe Acrobat - View as HTML
Page 1. Generic GF(2 m) Arithmetic in Software and its Application to ECC Andre Weimerskirch 1 , Douglas Stebila 2 , and Sheueling Chang Shantz 3 ...
www.crypto.ruhr-uni-bochum.de/imperia/ md/content/texte/weimerskirchetal_ecc.pdf - Similar pages

[PDF] **Efficient Arithmetic on Koblitz Curves ***
File Format: PDF/Adobe Acrobat
... Boston. Manufactured in The Netherlands. **Efficient Arithmetic on Koblitz Curves *** JEROME A. SOLINAS National Security Agency, Ft. ...
www.ingentaconnect.com/content/ klu/desi/2000/00000019/F0020002/00253940 - Similar pages

Goooooogle ▶
Result Page: 1 2 3 4 5 6 **Next**

"efficient arithmetic on koblitz cur Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Your search matched **3** documents.

A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 **Experimental results of covert channel limitation in one-way communication systems**
Ogurtsov, N.; Orman, H.; Schroeppel, R.; O'Malley, S.; Spatscheck, O.;
Network and Distributed System Security, 1997. Proceedings., 1997 Symposi
on , 10-11 Feb. 1997
Pages:2 - 15

[Abstract] [PDF Full-Text (1268KB)] **IEEE CNF**

2 **Parallelized network security protocols**
Nahum, E.; Yates, D.J.; O'Malley, S.; Orman, H.; Schroeppel, R.;
Network and Distributed System Security, 1996., Proceedings of the Symposi
on , 22-23 Feb. 1996
Pages:145 - 154

[Abstract] [PDF Full-Text (804KB)] **IEEE CNF**

3 **Towards High Performance Cryptographic Software**
Nahum, E.; O'Malley, S.; Orman, H.; Schroeppel, R.;
Architecture and Implementation of High Performance Communication Subsys
1995. (HPCS '95), 1995 Third IEEE Workshop on the , August 23-25, 1995
Pages:69 - 72

[Abstract] [PDF Full-Text (396KB)] **IEEE CNF**